SUSE

21.08.2024

Securing the cloud

2024 Edition
An industry trend report on cloud security challenges in the era of AI

Index

Executive summary

At SUSE, we recognize that every business is on a journey of digital transformation, and that transformation is enhanced and accelerated by open source software. This second edition of the 'Securing the cloud' trend report investigates how IT teams manage and think about cloud security, focusing on two major additional themes that have a profound impact on cloud security – GenerativeAI and Edge computing.

This report considers how the widespread use of increasingly complex cloud environments poses significant challenges, ranging from edge security to AI-powered cyberattacks, as well as examining how professionals are facing these challenges.

The findings of this report indicate that the adoption of cloud and cloud native technologies continues to face security challenges, with ransomware attacks, GenAI privacy and data security, and AI-powered cyberattacks seen as significant risks. A striking difference to last year's report is just how quickly generative AI has increased as a threat factor in cloud security.

Interestingly, the results reveal that cloud security incidents have decreased from last year, with 70% of teams experiencing a cloud security incident over the last 12 months (compared to 88% the year prior). While this may indicate the effectiveness of cloud security measures implemented by IT decision makers, of those that experienced an incident, 70% experienced multiple incidents, and 4% had more than 10 issues over the past year (down from 11% last year), highlight- ing the continued need for strong investment and vigilance.

Still, concerns about security holding back cloud technologies persist, as a further **86% of professionals agree that their teams would migrate more workloads to the cloud and to the edge if they knew their data couldn't be tampered with.** Additionally, 90% of software engineers have experienced an edge security event in the past year, the highest share out of all respondents' roles.

SUSE is exceptionally well-prepared to support businesses which are choosing open source and looking to transform with the cloud while remaining secure in times of GenAI and Edge computing. Cutting-edge companies are already entrusting SUSE with their mission critical needs.

Key findings

66% of IT decision makers are concerned about AI-powered cyberattacks

70% of teams have confirmed a cloud security incident over the last 12 months

62% of IT decision makers have experienced at least one edge security incident over the past year

33% of the work of those surveyed is in the cloud

86% of IT professionals would move more workloads to the cloud or edge if they knew it could not be tampered with

94% of IT decision makers intend to review their own software supply chain to increase security

46% of IT decision makers consider certifying processes and tools used to build software as a key measure to mitigate the risk and impact of supply chain attacks

GenAI security

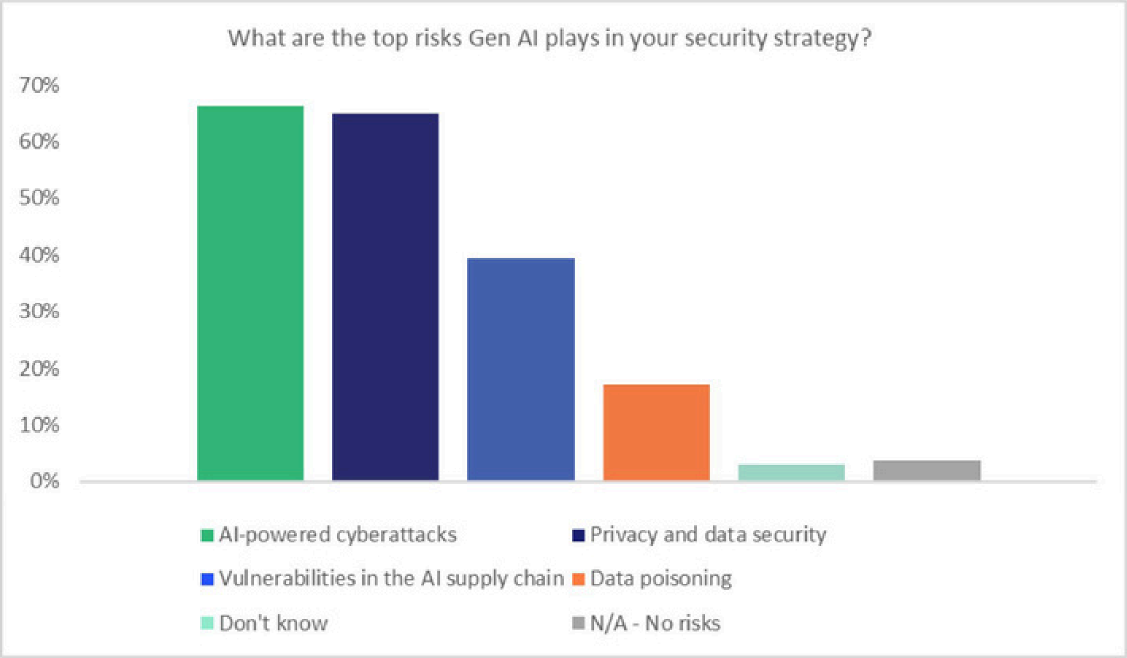
Generative AI emerges as a key security concern among IT decision makers, with threats perceived most strongly by US stakeholders.

AI-powered cyberattacks (66%) and privacy and data security (65%) are the top two concerns when it comes to generative AI cloud security. Only a small minority of IT decision makers did not believe there to be any risks related to the technology (4%).

Compared to Europe, concerns around GenAI security risks are much more prevalent in the US. Across all categories, incl. privacy and data security (73% vs. 62%), AI-powered cyberattacks (74% vs. 64%), vulnerabilities in the supply chain (50% vs. 36%) and data poisoning (25% vs. 14%), US respondents considered GenAI a higher risk in their security strategy.

Within European markets, privacy and data security were least considered a risk in the Netherlands (51%) and AI-powered cyber attacks were least considered a top risk in France (53%) and the Netherlands (56%).

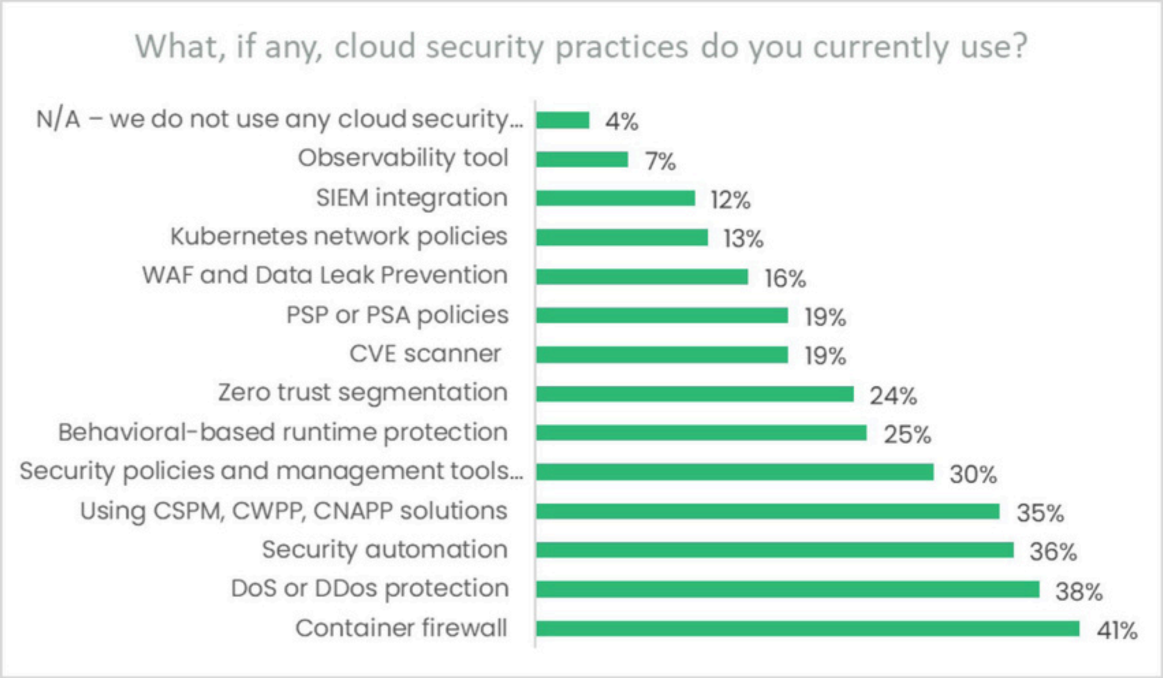
Among IT decision makers, software engineers (78%) were most concerned about privacy and data security, while network engineers (82%) were most concerned about AI-powered cyberattacks.



Security practices and budget

Majority of all IT decision makers have experienced at least one edge security incident in the last 12 months.

When it comes to the cloud security practices currently used, container firewall remains the most popular overall (41% vs. 38% in 2023), followed by DDos protection (38%) and security automation (36%). Interestingly, there are numerous cloud security practices that are significantly more popular amongst US-based IT decision makers compared to those in Europe, including behavioral-based runtime protection (32% in the US vs. 22% in Europe), security automation (47% in the US vs. 33% in Europe), CSPM, CWPP, CNAPP solutions (47% in the US vs. 31% in Europe), container firewall (47% in the US vs. 38% in Europe), and security policies and management tools provided by a Cloud vendor (39% in the US vs. 26% in Europe). Vice versa, DoS or DDoS protection is significantly more popular in Europe (41% in Europe vs. 29% in the US).



Edge security

A concerning 90% of software engineers have experienced an edge security event in the past year, the highest share out of all respondents' roles. The majority (62%) of all respondents had experienced at least one edge security incident. Germany (66%), the US (65%), and the Netherlands (64%) were the three most affected markets, followed by France (59%) and the UK (57%) as the least affected markets - although more than half were still affected by at least one incident.

In terms of edge computing security, respondents identified ensuring data privacy and compliance with regulations (37%) as the key challenge when managing and securing data at the edge. This was followed by ensuring reliable connectivity and data transfer

(30%) and integrating edge solutions with existing IT systems and managing and maintaining edge devices and infrastructure (both 28%).

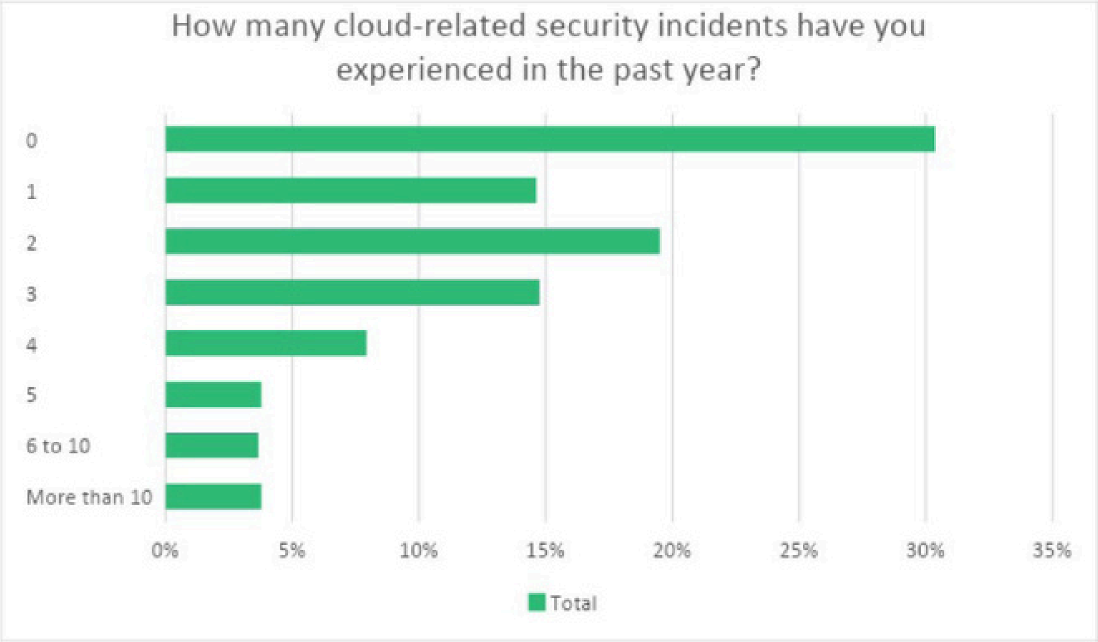
On average, those surveyed say they spend just over a third (30.2%) of their overall IT budget on cloud and cloud native security. This marks a decrease of 5.8% from last year. The US (36.5%) still spends a higher share of their budget on cloud and cloud native security compared to the EU (27.9%)

Incidents and concerns

On average, IT decision makers experience two cloud-related security incidents annually. Ransomware attacks are now the biggest concern.

On average, those surveyed say a third (33.1%) of their work is in the cloud – that is a slight uptick from the last year (32%). US-based IT decision makers (37.4%) still have a significantly greater proportion of their work in the cloud compared to those based in Europe (31.5%) -although the gap has narrowed from last year (37% vs. 29%).
IT decision makers reported, on average, 2.3 cloud-related security incidents in the past year, down from 4 last year. The country that was most affected were the Netherlands,(2.9 on average), with the UK (1.9 on average) being the least affected.

At a total level, the top cloud security concern is ransomware attacks (38%), followed by data theft and crypto mining within clusters, attacks on running services using unknown vulnerabilities, visibility and controls to sensitive data being accessed in the cloud, and monitor and alert on malicious activities behaviors (all 24%). Concerns around ransomware attacks vary considerably by market, with much stronger concerns in the UK and the US (both 43%) compared to France (29%).



Supply chain security

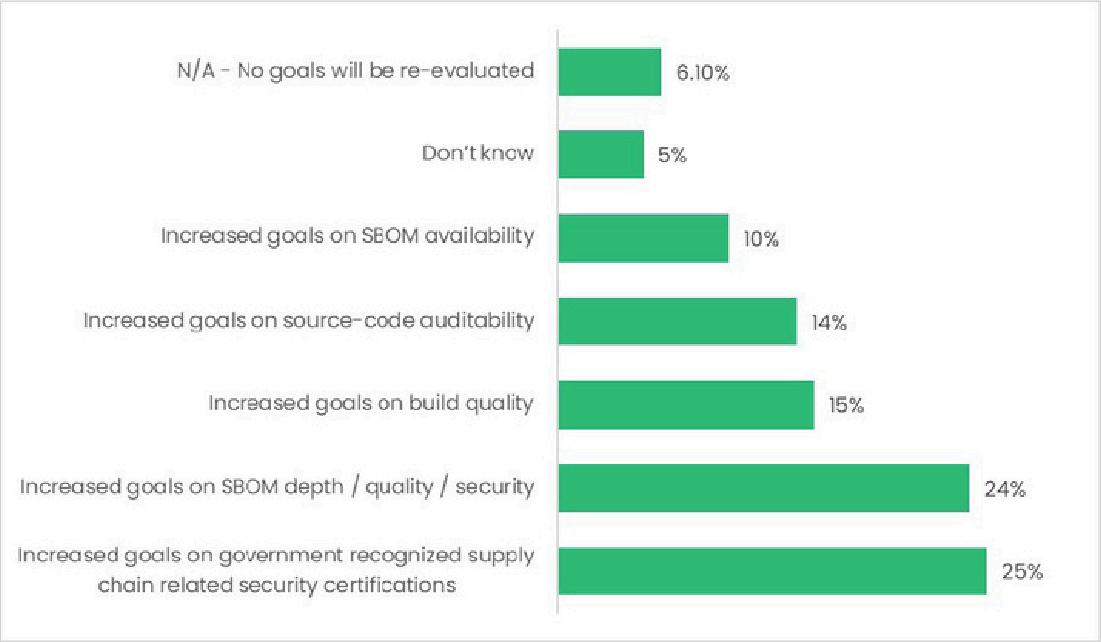
In-house auditing of vendors' software is considered the most important measure to mitigate risk and impact of supply chain attacks.

One in four IT decision makers believe that government-recognized supply chain related security certifications (25%) will become more of a priority for them over the next 12 months. IT decision makers also believe that source-code auditability (14%), build quality (15%), or SBOM depth / quality / security (24%) will be re-evaluated upward in the next years to become more of a priority.

IT decision makers living in the US and Europe believe that goals on source-code auditability (14%) will be re-evaluated, with the lowest share in Germany (11%) and the highest in the Netherlands (19%), followed by France (17%). Similarly, when asked about the re-evaluation of SBOM depth / quality / security, respondents in the US (20%) and Germany (20%) saw eye-to-eye. Europe as a group attributed it a higher likelihood (26%) with the UK (30%) being strongest in agreement.

Whether IT decision makers will need to re-evaluate the build quality of their software supply chains remains a divisive matter. However, while last year's European respondents were more likely (40%) to believe this as compared to US respondents (15%), this year roles were reversed with more decision makers from the US (24%) believing it to be the case compared to Europe (12%).

The data further varies with respondents' present role in the business. For example, those working as software / network engineers, technical architects, or developers are more likely to believe that goals on source-code auditability will be re-evaluated (24% vs. 14% average), but less likely to think that goals on SBOM depth / quality / security will be re-evaluated (20% vs. 23% average).



Considering recent regulatory changes, the majority (94%) of respondents intend to review their own software supply chain to increase security.

To mitigate the risk and impact of supply chain attacks, the most popular measures included certifying processes and tools used to build software (46%), leveraging software that is backed by principal vendors (44%) and in-house auditing of vendors software (43%). Certifying processes and tools used to build software is considered more important in the US (59%) compared to Europe (41%). In-house auditing of vendors software is a significantly more popular measure in Germany (53%) compared to the UK and the Netherlands (both 38%), with France at the average (43%).

Methodology

The 2024 edition of this trend report is based on a survey of 820 IT engineers, architects, developers, security managers, and directors. It takes a global perspective by polling quantitatively and qualitatively across the US, Germany, UK, France and the Netherlands.

It compares how professionals in each of these markets may differ in their approach to cloud and cloud native technologies, while revealing the state of adoption. The seniority of those polled ranges from C-Suite to IT decision makers.

Like the first edition of the report, which was published in 2023, it explores the regulatory push for supply chain security, identifies potential areas that may become higher priorities in the next 12 months, and delves into organizations' intentions to review their own software supply chain for increased security. Additionally, it investigates the prevalence of cloud workloads, cloud-related security incidents, and major cloud security concerns. As an addition to last year's report, it also introduces questions around Generative AI security.
It touches upon the importance of skills, tools, data integrity, and open source platforms in addressing security gaps and decision-making regarding cloud migration. It concludes with an inquiry into the percentage of IT spending allocated to cloud and cloud native security and current cloud security practices employed by organizations.

2024

SUSE Software Solutions
Germany GmbH

Frankenstraße 146
90461 Nürnberg
Germany

www.suse.com

For more information, contact SUSE at:

+1 800 796 3700 (U.S./Canada)

+49 (0)911-740 53-0 (Worldwide)

Thank You